(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
8 avril 2004 (08.04.2004)

PCT

(10) Numéro de publication internationale
WO 2004/029873 A1

(51) Classification internationale des brevets[7] :
G06K 19/073

(21) Numéro de la demande internationale :
PCT/FR2003/002780

(22) Date de dépôt international :
22 septembre 2003 (22.09.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/11879 25 septembre 2002 (25.09.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **OBERTHUR CARD SYSTEMS SA** [FR/FR]; 102, boulevard Malesherbes, F-75017 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **DISCHAMP, Paul** [FR/FR]; 26, rue Saint Lambert, F-75015 Paris (FR). **GIRAUD, Christophe** [FR/FR]; 7, Rue Fustel de Coulanges, F-75005 Paris (FR).

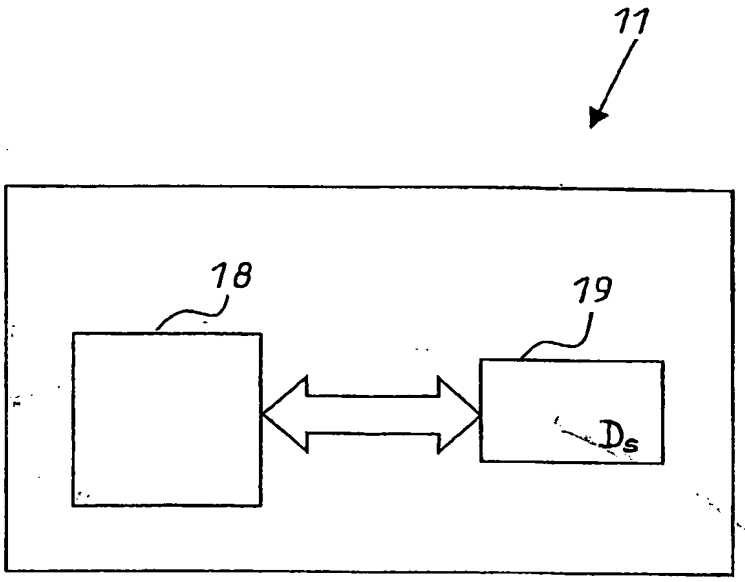
(74) Mandataire : **SANTARELLI**; 14, avenue de la Grande-Armée, Boîte postale 237, F-75822 Paris Cedex 17 (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: SECURE ELECTRIC UNIT COMPRISING TIME MANAGEMENT SYSTEM

(54) Titre : ENTITE ELECTRIQUE SECURISEE AVEC GESTION DU TEMPS



(57) Abstract: The invention relates to a secure electronic unit (11) comprising a means (18) of measuring the elapsed time between two operations. The invention also comprises means (19) of storing an authorised minimum or maximum duration, which co-operates with the aforementioned time measurement means (18) in order to determine if the elapsed time complies with the authorised duration. The invention is suitable, in particular, for SIM card- or bank card-type microcircuit cards.

[Suite sur la page suivante]

WO 2004/029873 A1

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) **Abrégé :** Entité électronique sécurisée (11) contient une unité (18) de mesure du temps qui s'écoule entre deux opérations. Elle comporte une unité (19) de mémorisation d'une durée minimale ou maximale autorisée, coopérant avec l'unité (18) de mesure du temps en vue de déterminer si le temps écoulé respecte la durée autorisée. Applications notamment aux cartes à microcircuit du type cartes bancaires ou cartes SIM.

ENTITE ELECTRONIQUE SECURISEE AVEC GESTION DU TEMPS

L'invention se rapporte à une entité électronique sécurisée et a notamment pour objet un perfectionnement apporté à une telle entité électronique pour que celle-ci puisse effectuer une gestion du temps qui s'écoule entre deux opérations et, à partir de l'élaboration d'une indication représentative du temps écoulé, contrôler si le temps écoulé respecte une durée autorisée minimale ou maximale entre deux opérations.

Dans toute la suite, les opérations considérées ne sont pas nécessairement de même nature.

On entend ici une gestion du temps "dans" la carte au sens où cette gestion est indépendante de tout système extérieur de mesure du temps, qu'il s'agisse par exemple d'un générateur de signal d'horloge ou de tout autre moyen de mesure du temps situé à l'extérieur par rapport à la carte.

Ces spécificités permettent de rendre relativement inviolable l'entité électronique objet de la présente invention.

L'invention peut s'appliquer à toute entité électronique sécurisée, comme, par exemple, une carte à microcircuit sécurisée, comportant des moyens lui permettant d'être couplée au moins temporairement à une source d'énergie électrique pour la mise en œuvre au moins d'une opération. L'invention peut notamment permettre de déterminer le temps qui s'écoule entre deux opérations, la connaissance de cette donnée supplémentaire permettant de détecter une tentative de fraude et, par conséquent, de sécuriser davantage l'entité électronique.

Par "opération", on entend de façon très générale toute étape mise en œuvre par l'entité électronique en question, que cette étape implique ou non un échange de données avec l'extérieur de l'ensemble constitué par la carte et son lecteur, voire la carte seule.

La sécurité d'une entité électronique (par exemple une carte à microcircuit telle qu'une carte bancaire ou une carte de contrôle d'accès ou autre) peut être améliorée s'il est possible de prendre en compte le temps qui s'est écoulé entre deux opérations.

Il existe une grande variété d'attaques possibles contre les cartes à microcircuit. Certaines de ces attaques ont pour but de retrouver les secrets qui sont conservés dans la mémoire du microcircuit ou de modifier le comportement normal de la carte afin d'en tirer profit. Par exemple, DPA (analyse de puissance différentielle, en anglais "*Differential Power Analysis*"), SPA (analyse de puissance simple, en anglais "*Simple Power Analysis*"), EMA (analyse électromagnétique, en anglais "*ElectroMagnetic Analysis*"), DEMA (analyse électromagnétique différentielle, en anglais "*Differential ElectroMagnetic Analysis*"), ou encore DFA (analyse d'erreur différentielle, en anglais "*Differential Fault Analysis*") sont des appellations bien connues de telles attaques, dites non intrusives, car n'entraînant pas la destruction de la carte.

Pour réaliser ces types d'attaques, il est généralement demandé à la carte d'exécuter des parties d'algorithmes de façon répétitive. Par exemple, pour retrouver des clés secrètes d'authentification de la carte au moyen d'une attaque DPA, il est habituellement demandé à la carte de s'authentifier n fois de suite, n étant un entier en général supérieur à 50. Ce grand nombre d'authentifications effectuées en très peu de temps est en principe une utilisation anormale de la carte.

Cependant, dans les cartes à microcircuit connues, la notion de temps est le plus souvent apportée par l'extérieur (comme, de façon classique, par un signal d'horloge extérieur), ce qui rend plus facilement réalisables les attaques mentionnées précédemment.

La présente invention a pour but de remédier aux inconvénients précités, en empêchant un "attaquant" ou un fraudeur d'utiliser de façon anormale une entité électronique sécurisée et en intégrant, pour ce faire, dans l'entité électronique, la gestion du temps entre deux opérations.

L'invention se propose ainsi de contraindre l'entité électronique à ne pas exécuter plus d'un certain nombre d'opérations en un temps donné.

Dans ce but, l'invention propose une entité électronique sécurisée, remarquable en ce qu'elle contient une unité de mesure du temps qui s'écoule entre deux opérations, et en ce qu'elle comporte une unité de mémorisation d'une durée minimale ou maximale autorisée, l'unité de mémorisation coopérant

avec l'unité de mesure du temps, en vue de déterminer si ce temps écoulé respecte cette durée autorisée.

Conformément à l'invention, les moyens permettant de déterminer le temps qui s'écoule entre deux opérations se situent dans l'entité électronique, ce qui permet d'augmenter sa sécurisation.

Avantageusement, l'unité de mesure du temps est adaptée à fournir une mesure du temps qui s'écoule entre deux opérations même lorsque l'entité électronique n'est pas alimentée par une source d'énergie extérieure.

Avantageusement, l'unité de mesure du temps est adaptée à fournir une mesure du temps qui s'écoule entre deux opérations même lorsque l'entité électronique n'est pas alimentée électriquement.

Avantageusement, l'unité de mesure du temps est adaptée à fournir une mesure du temps qui s'écoule entre deux opérations indépendamment de tout signal d'horloge extérieur.

En ce sens, l'entité électronique est autonome, à la fois du point de vue de la mesure du temps et du point de vue de l'alimentation électrique.

En variante, on peut bien entendu prévoir une pile et/ou une horloge dans l'entité électronique.

Les opérations dont il est question peuvent toutes être de même nature ; il peut s'agir, par exemple, uniquement d'opérations d'authentification. Cela n'est néanmoins pas toujours le cas et les opérations peuvent être de natures diverses.

L'unité de mesure du temps peut comporter un moyen de comparaison de deux dates, une date étant, de façon générale, une expression du temps courant et ces deux dates s'entendant ici comme deux instants définis par rapport à une même référence temporelle.

L'unité de mémorisation de la durée autorisée comporte avantageusement une entité sécurisée et peut être située dans ou hors de l'entité électronique.

Les "opérations" mentionnées ci-dessus peuvent comporter l'utilisation d'une donnée secrète, qui peut être par exemple une clé cryptographique ou un code personnel.

Dans une pluralité d'exemples d'application de l'invention, dont certains sont détaillés plus loin, la durée autorisée mentionnée ci-dessus correspond à une consommation maximale autorisée par unité de temps.

Dans un mode de réalisation préféré de la présente invention, l'entité électronique sécurisée comporte au moins un sous-ensemble comprenant :

un composant capacitif présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ce composant capacitif à une source d'énergie électrique pour être chargé par la source d'énergie électrique et

un moyen de mesure de la charge résiduelle du composant capacitif, cette charge résiduelle étant au moins en partie représentative du temps qui s'est écoulé après que le composant capacitif a été découplé de la source d'énergie électrique.

Dans ce cas, le composant capacitif du sous-ensemble précité ne peut être chargé que lorsque l'entité électronique sécurisée est couplée à la source d'énergie électrique. Cette dernière peut être extérieure à l'entité électronique sécurisée, mais ce n'est pas impératif : en variante, on peut prévoir d'alimenter l'entité électronique par une pile disposée dans ou sur celle-ci.

L'entité électronique pourra être pourvue d'un moyen de commutation pour découpler le composant capacitif de la source d'énergie électrique, cet événement initialisant la mesure du temps.

Plus généralement, la mesure du temps, c'est-à-dire la variation de charge du composant capacitif, commence dès que, après avoir été chargé, celui-ci se trouve électriquement isolé de tout autre circuit et ne peut plus se décharger qu'à travers son propre espace diélectrique.

Cependant, même si, physiquement, la charge résiduelle mesurée est liée à l'intervalle de temps écoulé entre l'isolement de l'élément capacitif et une mesure donnée de sa charge résiduelle, un intervalle de temps mesuré (qui sera considéré comme normal ou anormal ou qui pourra de toute façon être pris en compte pour déterminer si l'utilisation qui est faite de l'entité électronique est normale ou anormale) peut être déterminé entre deux mesures, la première mesure déterminant en quelque sorte une charge résiduelle de référence. Le moyen de mesure de la charge résiduelle du composant capacitif est mis en œuvre lorsqu'on désire connaître un temps écoulé.

Le composant capacitif étant chargé au cours d'une opération, le moyen de mesure de la charge résiduelle est mis en œuvre au cours d'une telle opération pour fournir une information au moins en partie représentative du temps qui s'est écoulé depuis la dernière opération.

Par ailleurs, l'invention permet en outre à l'entité électronique sécurisée de continuer à mesurer le temps entre deux opérations même après que l'entité électronique a été temporairement alimentée en courant et qu'elle se trouve ensuite dépourvue de toute nouvelle alimentation électrique. L'invention ne nécessite donc pas d'utiliser une source d'énergie électrique en permanence.

Le moyen de mesure de la charge résiduelle peut être compris dans l'unité de mesure du temps mentionnée plus haut.

Dans le mode préféré de réalisation, le moyen de mesure de la charge résiduelle comprend un transistor à effet de champ dont la grille est connectée à une borne du composant capacitif, c'est-à-dire à une "armature" d'une capacité.

Une telle capacité peut être réalisée en technologie MOS et son espace diélectrique peut alors être constitué par un oxyde de silicium. Dans ce cas, il est avantageux que le transistor à effet de champ soit réalisé également en technologie MOS. La grille du transistor à effet de champ et l'"armature" du composant capacitif MOS sont reliées et constituent une sorte de grille flottante qui peut être connectée à un composant permettant d'injecter des porteurs de charge.

On peut aussi faire en sorte qu'il n'existe aucune connexion électrique à proprement parler avec l'environnement extérieur. La connexion de la grille flottante peut être remplacée par une grille de contrôle (électriquement isolée) qui vient charger la grille flottante, par exemple par effet tunnel ou par "porteurs chauds". Cette grille permet de faire transiter des porteurs de charge vers la grille flottante commune au transistor à effet de champ et au composant capacitif. Cette technique est bien connue des fabricants de mémoires de type EPROM ou EEPROM.

Le transistor à effet de champ et le composant capacitif peuvent constituer une unité intégrée dans un microcircuit compris dans l'entité électronique sécurisée ou faisant partie d'un autre microcircuit logé dans la même entité électronique sécurisée.

Pendant certaines opérations, lorsque l'entité électronique sécurisée est encore couplée à une source d'énergie électrique extérieure, le composant capacitif est chargé à une valeur prédéterminée, connue ou mesurée et mémorisée, et le moyen de mesure de la charge résiduelle est relié à une borne de ce composant capacitif.

A la fin de l'opération, le moyen de mesure de la charge résiduelle, notamment le transistor à effet de champ, n'est plus alimenté mais sa grille reliée à la borne du composant capacitif est portée à une tension correspondant à la charge de celui-ci.

Pendant toute la période de temps qui sépare deux opérations, le composant capacitif se décharge lentement au travers de son propre espace diélectrique de sorte que la tension appliquée sur la grille du transistor à effet de champ diminue progressivement.

Au moment où l'entité électronique est à nouveau connectée à une source d'énergie électrique pour la mise en œuvre d'une nouvelle opération, une tension électrique est appliquée entre le drain et la source du transistor à effet de champ. Ainsi, un courant électrique allant du drain vers la source (ou dans le sens contraire selon les cas) est engendré et peut être recueilli et analysé.

La valeur du courant électrique mesuré dépend des paramètres technologiques du transistor à effet de champ et de la différence de potentiel entre le drain et la source, mais aussi de la tension entre la grille et le substrat. Le courant dépend donc des porteurs de charge accumulés dans la grille flottante commune au transistor à effet de champ et au composant capacitif. Par conséquent, ce courant de drain est aussi représentatif du temps qui s'est écoulé entre les deux opérations.

Le courant de fuite d'une telle capacité dépend bien sûr de l'épaisseur de son espace diélectrique mais également de tout autre paramètre dit technologique tel que les longueurs et surfaces de contact des éléments du composant capacitif. Il faut également prendre en compte l'architecture tridimensionnelle des contacts de ces parties, qui peut induire des phénomènes modifiant les paramètres du courant de fuite (par exemple, modification de la valeur de la capacité dite tunnel). Le type et la quantité des dopants et des

défauts peuvent être modulés pour modifier les caractéristiques du courant de fuite.

Les variations de température ont aussi une influence, plus précisément la moyenne des apports d'énergie calorifique appliqués à l'entité électronique sécurisée entre deux opérations, c'est-à-dire pendant le temps qu'on cherche à déterminer. En fait, tout paramètre intrinsèque à la technologie MOS peut être source de modulation du processus de la mesure du temps. En ce qui concerne les apports calorifiques, cependant, si le diélectrique est d'épaisseur très faible (inférieure à 5 nanomètres), le sous-ensemble correspondant est pratiquement insensible à la température, mais la fuite, relativement importante, est telle qu'on ne peut mesurer que des périodes de temps relativement faibles, de l'ordre de quelques minutes ou moins. Un tel sous-ensemble à fuite élevée indépendante de la température, peut cependant être retenu pour la détection de certains types de fraude. Par exemple, ce type de composant capacitif peut permettre de détecter des tentatives d'authentifications successives très rapprochées dans le temps ou des opérations de chiffrement de données qui sont caractéristiques de certaines attaques dites DPA mentionnées ci-dessus.

Pour mesurer des temps plus longs, il est nécessaire d'utiliser un composant capacitif ayant un espace diélectrique d'épaisseur plus importante. Dans ce cas, la fuite est sensible aux variations de température.

Avantageusement, l'épaisseur de la couche isolante du transistor à effet de champ est notablement supérieure (par exemple environ trois fois supérieure) à l'épaisseur de la couche isolante du composant capacitif.

Quant à l'épaisseur de la couche isolante du composant capacitif, elle est avantageusement comprise entre 4 et 10 nanomètres.

Pour obtenir une information sensiblement uniquement représentative du temps, on peut prévoir, dans une variante de réalisation, au moins deux sous-ensembles tels que définis ci-dessus, exploités "en parallèle". Les deux composants capacitifs sensibles à la température sont définis avec des fuites différentes, toutes choses égales par ailleurs, c'est-à-dire que leurs espaces diélectriques (épaisseur de la couche d'oxyde de silicium) ont des épaisseurs différentes.

A cet effet, selon une disposition avantageuse de l'invention, l'entité électronique définie ci-dessus est remarquable en ce qu'elle comporte :

au moins deux sous-ensembles précités comprenant chacun :

un composant capacitif présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ce composant capacitif à une source d'énergie électrique pour être chargé par cette source d'énergie électrique et

un moyen de mesure de la charge résiduelle du composant capacitif, cette charge résiduelle étant au moins en partie représentative du temps qui s'est écoulé après que le composant capacitif a été découplé de la source d'énergie électrique,

ces sous-ensembles comprenant des composants capacitifs présentant des fuites différentes au travers de leurs espaces diélectriques respectifs,

et en ce que l'entité électronique sécurisée comporte en outre :

des moyens de traitement des mesures des charges résiduelles respectives de ces composants capacitifs, pour extraire de ces mesures une information sensiblement indépendante des apports calorifiques appliqués à l'entité électronique sécurisée pendant le temps écoulé entre deux opérations.

Par exemple, les moyens de traitement peuvent comporter un tableau de valeurs de temps mémorisées, ce tableau étant adressé par ces mesures respectives. Autrement dit, chaque couple de mesures désigne une valeur de temps mémorisée indépendante de la température et des variations de température pendant la période mesurée. L'entité électronique comporte avantageusement une mémoire associée à un microprocesseur et une partie de cette mémoire peut être utilisée pour mémoriser le tableau de valeurs.

En variante, les moyens de traitement peuvent comporter un logiciel de calcul programmé pour exécuter une fonction prédéterminée permettant de calculer l'information temps, sensiblement indépendante des apports calorifiques, en fonction des deux mesures précitées.

Dans un mode particulier de réalisation, l'unité de mémorisation est adaptée à mémoriser une durée de sécurité, pendant laquelle on met en œuvre un processus de sécurité prédéterminé lorsque le temps écoulé entre deux opérations ne respecte pas la durée minimale autorisée précitée.

Cela permet d'augmenter encore la sécurité de l'entité électronique.

L'invention est particulièrement adaptée à s'appliquer aux cartes à microcircuit. L'entité électronique sécurisée peut être une carte à microcircuit, ou en comprendre une, ou encore être d'un autre type, par exemple, être une carte PCMCIA (architecture internationale de cartes-mémoire d'ordinateurs individuels, en anglais "*Personal Computer Memory Card International Architecture*").

L'invention est en outre remarquable par son niveau d'intégration.

D'autres aspects et avantages de l'invention apparaîtront à la lecture de la description détaillée qui suit de modes particuliers de réalisation, donnés à titre d'exemples non limitatifs. La description est faite en référence aux dessins qui l'accompagnent, dans lesquels :

- la figure 1 est un synoptique représentant, dans un mode particulier de réalisation, une entité électronique sécurisée conforme à la présente invention ;
- la figure 2 est un schéma-bloc d'une carte à microcircuit à laquelle peut s'appliquer l'invention, dans un mode particulier de réalisation ;
- la figure 3 est un schéma de principe d'un sous-ensemble que l'entité électronique sécurisée peut comporter dans un mode particulier de réalisation ; et
- la figure 4 est un schéma-bloc d'une variante du mode de réalisation des figures 1 et 2.

Comme le montre la **figure 1**, une entité électronique sécurisée 11 conforme à la présente invention contient une unité 18 de mesure du temps qui s'écoule entre deux opérations.

L'unité 18 de mesure du temps est indépendante de tout système extérieur de mesure du temps, qu'il s'agisse par exemple d'un générateur de signal d'horloge ou de tout autre moyen de mesure du temps situé à l'extérieur par rapport à la carte.

Cette unité 18 de mesure du temps qui s'écoule entre deux opérations permet d'éviter qu'un éventuel attaquant ou fraudeur puisse acquérir des secrets, tels qu'une clé de chiffrement, qui sont mémorisés dans l'entité électronique 11, ou que l'attaquant puisse modifier le comportement de l'entité électronique 11 afin d'en tirer profit illégalement.

Pour cela, dans un premier exemple décrit ici à titre non limitatif, on contraint l'entité électronique sécurisée 11 à ne pas exécuter plus d'un certain nombre d'authentifications, ou d'autres fonctions faisant appel à des algorithmes cryptographiques, en un temps donné.

Certes, un comportement autorisé de l'entité électronique sécurisée 11 peut impliquer l'exécution de plusieurs authentifications en un temps donné. Cependant, ce nombre d'authentifications successives a une limite. Ainsi, par exemple, on peut prévoir que, si l'entité électronique sécurisée 11 effectue un nombre total N, à décider au préalable, d'authentifications en un intervalle de temps inférieur à une durée minimale autorisée T_{min1}, il soit nécessaire d'attendre un temps T_{att1} avant de pouvoir effectuer la $(N+1)^{ème}$ authentification, puis à nouveau T_{att1} minutes avant de pouvoir effectuer la $(N+2)^{ème}$, et ainsi de suite.

A titre d'exemple non limitatif, on peut choisir N = 50, T_{min1} = 5 minutes et T_{att1} = 10 minutes. L'enchaînement des opérations est alors le suivant : en cas de 50 authentifications en moins de 5 minutes, par exemple 3 minutes, on autorise une $51^{ème}$ authentification à la $13^{ème}$ minute, une $52^{ème}$ authentification à la $23^{ème}$ minute, une $53^{ème}$ authentification à la $33^{ème}$ minute, etc.

L'entité électronique sécurisée 11 comporte à cet effet une unité 19 de mémorisation d'une durée autorisée. Il peut s'agir, soit d'une durée minimale T_{min}, comme T_{min1} dans le premier exemple décrit ici, soit d'une durée maximale T_{max}. L'unité 19 de mémorisation de la durée autorisée est avantageusement une mémoire sécurisée de l'entité électronique 11, cette mémoire étant notamment non accessible de l'extérieur. En variante, on peut envisager de situer l'unité 19 de mémorisation de la durée autorisée hors de l'entité électronique sécurisée 11, dans une entité sécurisée extérieure. Dans ce dernier cas, la valeur de la durée autorisée T_{min} ou T_{max} est reçue de l'extérieur, de la part d'un tiers dit "de confiance" (autorité habilitée), par l'entité électronique sécurisée 11, par l'intermédiaire d'un protocole sécurisé (i.e. mettant en œuvre des moyens cryptographiques) et est mémorisée au moins temporairement dans une zone sécurisée de l'entité électronique 11.

Conformément à la présente invention, l'unité 19 de mémorisation coopère avec l'unité 18 de mesure du temps, en vue de déterminer si le temps écoulé entre les deux opérations respecte la durée autorisée T_{min} ou T_{max}.

On peut prévoir dans la mémoire de l'entité électronique sécurisée 11 une région (comprenant par exemple un fichier) contenant la date, par exemple en secondes, à partir d'une référence de temps initiale prédéterminée, des N dernières authentifications effectuées. La référence de temps initiale correspond à un instant donné de la vie de l'entité électronique tel que la fin de sa personnalisation, ou sa première mise sous tension, ou encore la dernière opération sur laquelle on a effectué la gestion du temps.

Dès lors, dans le premier exemple décrit ici, avant d'effectuer une nouvelle authentification, il est prévu, par exemple dans l'application considérée mise en œuvre par l'entité électronique sécurisée 11, de comparer la date de la $N^{ème}$ authentification avec la date de la première authentification. Si la différence entre les deux dates est supérieure à la durée minimale autorisée T_{min1}, l'authentification est effectuée normalement. En revanche, si la différence entre les deux dates est inférieure à la durée autorisée T_{min1}, on peut prévoir de démarrer un processus de sécurité P_{s1}, consistant par exemple à n'autoriser qu'une seule authentification par tranche de temps de T_{att1} pendant une durée de sécurité D_s.

Dans l'exemple non limitatif donné ci-dessus, on peut choisir D_s = 2 heures.

Après écoulement de la durée de sécurité D_s, le processus de sécurité P_{s1} s'arrête et l'entité électronique sécurisée 11 repasse en mode de fonctionnement normal.

Il est préférable de mettre à jour la région de mémoire (comprenant par exemple un fichier) contenant les données relatives au temps avant d'effectuer l'authentification, afin d'éviter une attaque qui pourrait empêcher l'écriture dans ce fichier.

Dans un deuxième exemple décrit ici à titre non limitatif, un autre processus de sécurité P_{s2} consiste à inclure un écart de temps T_{att2} croissant entre les opérations - par exemple les authentifications. Par exemple, on peut choisir un écart de temps T_{att2} qui suit une progression géométrique. Dans l'exemple donné ici, cet écart de temps est chaque fois doublé entre deux opérations.

Ainsi, les N premières authentifications peuvent être réalisées en un temps T_{min2}, puis, une fois le processus de sécurité P_{s2} déclenché, on initialise un compteur de temps (par exemple à une valeur $T_{att2} = T_0$) qui fixe le temps d'attente T_{att2} entre deux opérations, qui sont ici des authentifications. A chaque nouvelle authentification, la valeur courante T_{att2} de ce compteur de temps est multipliée par 2, c'est-à-dire que le temps d'attente entre les $1^{ère}$ et $N^{ème}$ opérations vaut T_0 et, pour tout entier i supérieur ou égal à 0, le temps d'attente entre les $(N+i)^{ème}$ et $(N+i+1)^{ème}$ opérations vaut $T_{att2} = 2^i \times T_0$.

A titre d'exemple non limitatif, on peut choisir N = 50, T_{min2} = 5 minutes et T_0 = 1 minute. L'enchaînement des opérations est alors le suivant : en cas de 50 authentifications en moins de 5 minutes, par exemple 4 minutes, on autorise une $51^{ème}$ authentification à la $5^{ème}$ minute, une $52^{ème}$ authentification à la $7^{ème}$ minute, une $53^{ème}$ authentification à la $11^{ème}$ minute, etc.

De même que dans le premier exemple décrit précédemment, après écoulement de la durée de sécurité D_s, le processus de sécurité P_{s2} s'arrête si aucune nouvelle authentification n'a eu lieu et l'entité électronique sécurisée 11 repasse en mode de fonctionnement normal.

Dans un troisième exemple décrit ici à titre non limitatif, un autre processus de sécurité P_{s3} consiste à bloquer l'entité électronique sécurisée 11 de façon définitive si un trop grand nombre d'opérations (dans cet exemple, des authentifications), i.e. un nombre d'opérations supérieur à un nombre maximal autorisé d'opérations défini préalablement, sont effectuées en un temps donné. Autrement dit, une durée minimale imposée entre deux opérations n'aura pas été respectée.

Par exemple, si N authentifications ont été réalisées en un temps inférieur à une durée minimale imposée T_{min3}, on peut considérer qu'il s'agit d'une utilisation anormale de l'application mise en œuvre par l'entité électronique sécurisée 11 et on oblige alors l'entité électronique 11 à se mettre définitivement hors service. Cet état peut être obtenu par exemple par effacement de toutes les données mémorisées.

A titre d'exemple non limitatif, on peut choisir N = 50 et T_{min3} = 5 minutes. Dans ce cas, l'entité électronique sécurisée 11 se bloque si 50 authentifications ont été réalisées en moins de 5 minutes.

On peut combiner les processus de sécurité P_{s1} et P_{s3}.

La **figure 2** illustre une entité électronique sécurisée 11 conforme à la présente invention, dans un mode particulier de réalisation où cette entité est une carte à microcircuit. L'entité électronique sécurisée 11 comporte une unité 12 lui permettant d'être couplée à une source d'énergie électrique extérieure 16.

Dans le mode particulier de réalisation représenté, l'entité électronique sécurisée 11 comporte des plages de raccordement métalliques susceptibles d'être connectées à une unité formant un lecteur de carte. Deux de ces plages de raccordement 13a, 13b sont réservées à l'alimentation électrique du microcircuit, la source d'énergie électrique étant logée dans un serveur ou autre dispositif auquel l'entité électronique sécurisée est momentanément raccordée. Ces plages de raccordement peuvent être remplacées par une antenne logée dans l'épaisseur de la carte et susceptible de fournir au microcircuit l'énergie électrique nécessaire à son alimentation tout en assurant la transmission bidirectionnelle de signaux radiofréquence permettant les échanges d'informations. On parle alors de technologie sans contact.

Le microcircuit comprend un microprocesseur 14 associé de façon classique à une mémoire 15.

Dans un exemple particulier de réalisation, l'entité électronique sécurisée 11 comporte au moins un sous-ensemble 17 (ou est associée à un tel sous-ensemble) chargé de la mesure du temps.

Le sous-ensemble 17, qui est représenté plus en détail sur la **figure 3**, est donc logé dans l'entité électronique sécurisée 11. Il peut faire partie du microcircuit et être réalisé dans la même technologie d'intégration que celui-ci.

Dans l'exemple, ce sous-ensemble 17 n'est relié à aucune source d'énergie électrique interne. Il ne peut donc être alimenté que lorsque l'entité électronique sécurisée 11 est effectivement couplée à un serveur ou à un lecteur de carte, comportant une telle source d'énergie électrique. Cependant, si l'entité électronique sécurisée 11 doit être alimentée en permanence, le sous-ensemble 17 qui est chargé de la mesure du temps peut être alimenté ou non via un module de commutation permettant de coupler l'entité électronique sécurisée 11 à la source d'énergie électrique ou de l'isoler de celle-ci. Un tel module de

commutation est par exemple partie intégrante du microprocesseur 14, ou constitué par des éléments de commutation gérés par le microprocesseur 14.

Le sous-ensemble 17 comprend un composant capacitif 20 présentant une fuite au travers de son espace diélectrique 24 et une unité 22 de mesure de la charge résiduelle de ce composant 20.

Cette charge résiduelle est au moins en partie représentative du temps écoulé après que le composant capacitif 20 a été découplé de la source d'énergie électrique, c'est-à-dire, dans l'exemple donné ici, entre deux opérations.

Le composant capacitif 20 est chargé par la source d'énergie électrique extérieure au cours d'une opération, soit par connexion directe, comme dans l'exemple décrit, soit par tout autre moyen qui peut amener à charger la grille. L'effet tunnel est une méthode permettant de charger la grille sans connexion directe. Dans l'exemple, la charge du composant capacitif 20 est pilotée par le microprocesseur 14.

Dans l'exemple, le composant capacitif 20 est une capacité réalisée suivant la technologie MOS. L'espace diélectrique 24 de cette capacité est constitué par une couche d'oxyde de silicium déposée à la surface d'un substrat 26 constituant une des armatures du condensateur. Ce substrat 26 est ici connecté à la masse, c'est-à-dire à une des bornes d'alimentation de la source d'énergie électrique extérieure, lorsque celle-ci se trouve raccordée à la carte. L'autre armature du condensateur est un dépôt conducteur 28a appliqué sur l'autre face de la couche d'oxyde de silicium.

Par ailleurs, l'unité 22 de mesure mentionnée précédemment comprend essentiellement un transistor 30 à effet de champ, ici réalisé suivant la technologie MOS, comme la capacité. La grille du transistor 30 est connectée à une borne du composant capacitif 20. Dans l'exemple, la grille est un dépôt conducteur 28b de même nature que le dépôt conducteur 28a qui, comme indiqué ci-dessus, constitue une des armatures du composant capacitif 20.

Les deux dépôts conducteurs 28a et 28b sont reliés l'un à l'autre ou ne constituent qu'un seul et même dépôt conducteur. Une connexion 32 reliée au microprocesseur 14 permet d'appliquer une tension à ces deux dépôts 28a et

28b, pendant un court intervalle de temps nécessaire pour charger le composant capacitif 20. L'application de cette tension est pilotée par le microprocesseur 14.

Plus généralement, la connexion 32 permet de charger le composant capacitif 20 à un moment choisi, sous la commande du microprocesseur 14 et c'est à partir du moment où cette connexion de charge est coupée par le microprocesseur 14 (ou lorsque l'entité électronique sécurisée 11 est découplée dans son ensemble de toute source d'alimentation électrique) que la décharge du composant capacitif 20 au travers de son espace diélectrique 24 commence, cette perte de charge électrique étant représentative du temps écoulé. La mesure du temps implique la mise en conduction momentanée du transistor 30, ce qui suppose la présence d'une source d'énergie électrique appliquée entre drain et source.

Le transistor 30 à effet de champ en technologie MOS comporte, outre la grille, un espace diélectrique de grille 34 séparant cette dernière d'un substrat 36 dans lequel sont définies une région de drain 38 et une région de source 39. L'espace diélectrique de grille 34 est constitué par une couche isolante d'oxyde de silicium. La connexion de source 40 appliquée à la région de source 39 est reliée à la masse et au substrat 36. La connexion de drain 41 est reliée à un circuit de mesure du courant de drain qui comporte une résistance 45 aux bornes de laquelle sont connectées les deux entrées d'un amplificateur différentiel 46. La tension délivrée à la sortie de cet amplificateur est donc proportionnelle au courant de drain.

La grille 28b est mise en position flottante pendant le temps qui s'écoule entre deux couplages ou connexions à une source d'énergie électrique extérieure, c'est-à-dire à l'occasion de deux opérations successives. Autrement dit, aucune tension n'est appliquée à la grille pendant cet intervalle de temps. En revanche, puisque la grille est connectée à une armature du composant capacitif 20, la tension de grille pendant cet intervalle de temps est égale à une tension qui se développe entre les bornes du composant capacitif 20 et qui résulte d'une charge initiale de celui-ci réalisée sous le contrôle du microprocesseur 14 au cours de la dernière opération.

L'épaisseur de la couche isolante du transistor 30 est notablement plus grande que celle du composant capacitif 20. A titre d'exemple non limitatif,

l'épaisseur de la couche isolante du transistor 30 peut être environ trois fois supérieure à l'épaisseur de la couche isolante du composant capacitif 20. Selon l'application envisagée, l'épaisseur de la couche isolante du composant capacitif 20 est comprise entre 4 et 10 nanomètres, environ.

Lorsque le composant capacitif 20 est chargé par la source d'énergie électrique extérieure et après que la connexion de charge a été coupée sous la commande du microprocesseur 14, la tension aux bornes du composant capacitif 20 diminue lentement au fur et à mesure que ce dernier se décharge progressivement au travers de son propre espace diélectrique 24. La décharge au travers de l'espace diélectrique 34 du transistor 30 à effet de champ est négligeable compte tenu de l'épaisseur de ce dernier.

A titre d'exemple nullement limitatif, si, pour une épaisseur d'espace diélectrique donnée, on charge la grille et l'armature du composant capacitif 20 à 6 volts à un instant t = 0, le temps associé à une perte de charge de 1 volt, c'est-à-dire un abaissement de la tension à une valeur de 5 volts, est de l'ordre de 24 secondes pour une épaisseur de 8 nanomètres.

Pour des épaisseurs différentes, on peut dresser le tableau suivant :

Durée	1 heure	1 journée	1 semaine	1 mois
Epaisseur d'oxyde	8,17 nm	8,79 nm	9,17 nm	9.43 nm
Précision sur le temps	1,85 %	2,09 %	2,24 %	3,10 %

La précision dépend de l'erreur commise sur la lecture du courant de drain (0,1 % environ). Ainsi, pour pouvoir mesurer des temps de l'ordre d'une semaine, on peut prévoir une couche d'espace diélectrique de l'ordre de 9 nanomètres.

La figure 3 montre une architecture particulière qui utilise une connexion directe à la grille flottante (28a, 28b) pour y appliquer un potentiel électrique et donc y faire transiter des charges. On peut aussi procéder à une charge indirecte, comme mentionné précédemment, grâce à une grille de contrôle remplaçant la connexion directe, selon la technologie utilisée pour la fabrication des cellules EPROM ou EEPROM.

La variante de la **figure 4** prévoit trois sous-ensembles 17A, 17B, 17C, chacun associé au microprocesseur 14. Les sous-ensembles 17A et 17B comprennent des composants capacitifs présentant des fuites relativement faibles pour permettre des mesures de temps relativement longs.

Cependant, ces composants capacitifs sont généralement sensibles aux variations de température. Le troisième sous-ensemble 17C comporte un composant capacitif présentant un espace diélectrique très faible, inférieur à 5 nanomètres. Il est de ce fait insensible aux variations de température. Les deux composants capacitifs des sous-ensembles 17A, 17B présentent des fuites différentes au travers de leurs espaces diélectriques respectifs.

En outre, l'entité électronique sécurisée comporte un module de traitement des mesures des charges résiduelles respectives présentes dans les composants capacitifs des deux premiers sous-ensembles 17A, 17B. Ce module de traitement est adapté à extraire de ces mesures une information représentative des temps et sensiblement indépendante des apports calorifiques appliqués à l'entité électronique sécurisée pendant le temps écoulé entre deux opérations successives précitées.

Dans l'exemple, ce module de traitement se confond avec le microprocesseur 14 et la mémoire 15. En particulier, un espace de la mémoire 15 est réservé à la mémorisation d'un tableau T à double entrée de valeurs de temps et ce tableau est adressé par les deux mesures respectives issues des sous-ensembles 17A et 17B. Autrement dit, une partie de la mémoire comporte un ensemble de valeurs de temps et chaque valeur correspond à un couple de mesures résultant de la lecture du courant de drain de chacun des deux transistors des sous-ensembles 17A, 17B sensibles à la température.

Ainsi, pendant une opération, par exemple vers la fin de celle-ci, les deux composants capacitifs sont chargés, à une valeur de tension prédéterminée, par la source d'énergie électrique extérieure, via le microprocesseur 14. Lorsque la carte à microcircuit est découplée du serveur ou lecteur de carte ou autre entité, les deux composants capacitifs restent chargés mais commencent à se décharger au travers de leurs propres espaces diélectriques respectifs et, au fur et à mesure que le temps s'écoule, sans que la carte à microcircuit soit utilisée, la charge résiduelle de chacun des composants capacitifs décroît mais

différemment dans l'un ou l'autre, en raison des fuites différentes déterminées par construction.

Lorsque la carte est à nouveau couplée à une source d'énergie électrique extérieure à l'occasion d'une nouvelle opération, les charges résiduelles des deux composants capacitifs sont représentatives du même intervalle de temps qu'on cherche à déterminer mais diffèrent en raison des variations de température qui ont pu se produire pendant toute cette période de temps.

Au moment de la réutilisation de la carte, les deux transistors à effet de champ de ces deux sous-ensembles sont alimentés et les valeurs des courants de drain sont lues et traitées par le microcircuit. Pour chaque couple de valeurs de courant de drain, le microcircuit va chercher en mémoire, dans le tableau T mentionné précédemment, la valeur de temps correspondante. Cette valeur de temps est alors comparée à la durée minimale ou maximale autorisée et l'opération n'est autorisée que si le temps écoulé est, selon l'application considérée, supérieur à la durée minimale autorisée, ou inférieur à la durée maximale autorisée, respectivement.

En variante, cette valeur de temps peut être comparée avec une valeur disponible dans le serveur ou lecteur de carte ou autre entité, de préférence sécurisée. De plus, l'opération peut n'être autorisée que si, non seulement le temps écoulé respecte la durée minimale ou maximale autorisée, mais si en outre, la valeur de temps obtenue dans la carte (par exemple la valeur de temps mémorisée dans le tableau T) est compatible avec la valeur disponible dans le serveur ou lecteur de carte ou autre entité, c'est-à-dire si en outre ces deux valeurs coïncident ou sont relativement proches, selon une tolérance choisie au préalable.

Il n'est pas nécessaire de mémoriser le tableau T. Par exemple, le module de traitement, c'est-à-dire essentiellement le microprocesseur 14, peut comporter une partie de logiciel de calcul d'une fonction prédéterminée permettant de déterminer ladite information sensiblement indépendante des apports calorifiques en fonction des deux mesures.

Le troisième sous-ensemble 17C comporte, comme décrit plus haut, un espace diélectrique extrêmement mince le rendant insensible aux variations de température. Ce sous-ensemble peut être utilisé, sous le contrôle du

microprocesseur 14, pour détecter des tentatives d'authentification répétées qui par exemple se produisent souvent lors d'une attaque de type DPA.

D'autres variantes sont possibles. En particulier, si on veut simplifier le sous-ensemble 17, on peut envisager de supprimer le composant capacitif 20 en tant que tel, car le transistor 30 à effet de champ peut lui-même être considéré comme un composant capacitif avec la grille 28b et le substrat 36 en tant qu'armatures, ces dernières étant séparées par l'espace diélectrique 34. Dans ce cas, on peut considérer que le composant capacitif et l'unité de mesure sont confondus.

Dans les trois exemples décrits plus haut incluant la mise en œuvre de processus de sécurité P_{s1}, P_{s2} et P_{s3}, il y a plusieurs possibilités pour conserver l'indication de temps entre les opérations.

Une première possibilité consiste à charger la cellule qui mesure le temps une fois, lors de la mise en service de la carte. Lorsqu'une opération (par exemple une authentification) est effectuée, l'état de la charge de la cellule à un instant t1 est mémorisé (par exemple inscrit dans un fichier d'une région sécurisée de la mémoire de la carte). Lorsqu'une deuxième opération de même nature (dans l'exemple, une deuxième authentification) est effectuée, l'état de la charge de la cellule à l'instant t2 est mémorisé (dans l'exemple, inscrit dans le fichier), et ainsi de suite, de façon que, lorsqu'une $N^{ème}$ opération de même nature (dans l'exemple, avec N = 50, une $50^{ème}$ authentification) est effectuée, l'état de la charge de la cellule à l'instant tN est mémorisé (dans l'exemple, t50 est inscrit dans le fichier).

Pour déterminer le temps écoulé entre la $1^{ère}$ et la $N^{ème}$ opérations, il suffit de comparer l'état de la charge de la cellule à t1 à l'état de la charge de la cellule à tN. Par soustraction des valeurs des charges et par l'intermédiaire d'une table de correspondance entre charges et temps écoulé (pouvant être élaborée à partir d'un tableau analogue au tableau T décrit plus haut), on obtient le temps écoulé recherché.

En effet, par "charge" de la cellule, on entend ici la valeur physique liée à cette cellule, telle que la tension à ses bornes. Néanmoins, pour une utilisation plus simple de cette grandeur, on peut prévoir dans la carte un système (comme par exemple la table de correspondance mentionnée ci-dessus) permettant

d'associer cette valeur physique à une grandeur logique plus directement représentative du temps.

D'autres possibilités consistent à recharger la cellule à intervalles de temps réguliers, ou encore à chaque mise sous tension de l'entité électronique sécurisée.

On utilise avantageusement un seul composant capacitif pour une pluralité d'opérations. A chaque exécution d'une opération donnée (par exemple, la mise à zéro de la carte), le temps écoulé depuis la dernière recharge du composant capacitif est mesuré, puis le composant capacitif est rechargé. On accumule les temps ainsi mesurés dans un emplacement de la mémoire non volatile de la carte.

Cet emplacement mémoire mémorise ainsi le temps écoulé depuis la première charge du composant capacitif (la première charge ayant lieu, par exemple, lors de la première mise sous tension de la carte) et permet de connaître le temps écoulé à tout moment pour tout type d'opération.

Cette solution a pour avantage d'utiliser un seul composant capacitif ayant une épaisseur d'oxyde relativement faible, ce qui confère une plus grande précision dans la mesure du temps, par comparaison avec le cas d'un seul composant pour toute la durée de vie de la carte.

Le temps qui s'écoule entre l'instant de mesure de la charge du composant capacitif et le moment de sa recharge est parfois non négligeable, en particulier si la carte est retirée du lecteur avant recharge. Pour prendre en compte cet intervalle de temps, on peut utiliser un second composant dont la fonction sera de prendre le relais du premier pendant cet intervalle de temps.

On peut également prévoir d'utiliser des composants capacitifs de précisions différentes afin d'améliorer la précision de la mesure : on choisira, parmi plusieurs mesures, celle obtenue à partir du composant le plus précis qui n'est pas déchargé.

Encore une autre possibilité consiste à recharger la cellule à chaque exécution d'une opération d'un type donné (par exemple, à chaque authentification), après avoir mesuré le temps écoulé depuis la précédente opération du même type. Un avantage de cette possibilité est qu'on peut prévoir des composants adaptés à l'opération à contrôler, pour améliorer la précision de

la mesure du temps ; dans la cellule de mesure du temps, en particulier pour ce qui concerne l'épaisseur d'oxyde, on a vu par le tableau donné plus haut que le choix de l'épaisseur d'oxyde influe sur la précision de la mesure.

Cette possibilité de rechargement de la cellule à chaque exécution d'une opération d'un type donné est appropriée lorsqu'on prévoit une cellule de mesure du temps pour chaque application considérée dans la carte. En effet, sachant que la cellule est rechargée à chaque nouvelle opération de même nature, chaque application ayant recours au système de gestion du temps conforme à la présente invention utilise la cellule de mesure du temps qui lui est associée.

Dans cette hypothèse, pour l'application considérée, la différence entre la charge maximale de la cellule et l'état de la charge à l'instant de la nouvelle opération (dans l'exemple, la nouvelle authentification) est mémorisée (dans l'exemple, dans un fichier d'une région sécurisée de la mémoire de la carte). Cette différence représente le temps écoulé entre les deux opérations.

Pour obtenir le temps écoulé entre N opérations, il suffit alors d'additionner les (N-1) valeurs des différences précédemment mémorisées.

D'autres variantes, à la portée de l'homme du métier, sont possibles.

Un autre exemple d'application d'une entité électronique sécurisée conforme à la présente invention, dans lequel l'entité électronique est également une carte à microcircuit, consiste, dans le domaine bancaire, à introduire une sécurité supplémentaire pour les achats effectués au moyen de la carte.

Par exemple, on peut prévoir de déclencher une connexion avec le serveur de la banque concernée lorsque de nombreux achats de faibles montants auront été réalisés (généralement sans connexion à la banque) dans un intervalle de temps donné (par exemple dix "petits achats" en une heure). Le choix de cet intervalle de temps, i.e. de la durée autorisée au sens de la présente invention, peut dépendre de l'état du compte bancaire du porteur de la carte au moment où la carte a réalisé sa dernière connexion avec la banque.

Pour ce faire, dans un mode particulier de réalisation, la carte contient un fichier avec la date et le montant des achats. La date est mémorisée, par exemple, sous forme de l'état de la charge dans la cellule de mesure du temps, décrite plus haut en liaison avec les figures 2 à 4, ou bien mémorisée sous forme d'une valeur logique plus directement représentative du temps, dans une table

de correspondance entre charges et temps écoulé comme indiqué précédemment. Les opérations sont ici constituées par l'un quelconque des traitements récurrents effectués par la carte au cours d'un achat.

A chaque nouvel achat, l'application mise en œuvre par la carte va chercher toutes les opérations effectuées depuis écoulement d'un temps U_t et calculer le nombre total de "petits achats" effectués par l'utilisateur de la carte. Si ce nombre est inférieur à un seuil prédéfini autorisé dans l'intervalle de temps considéré, le nouvel achat est accepté ; sinon, la carte communique avec la banque l'ayant délivrée, à des fins de vérification.

Ainsi, conformément à l'invention, l'utilisation du compteur de temps à l'intérieur de la carte permet d'améliorer la sécurité puisque le décompte du temps est difficile à falsifier.

Un exemple d'application d'une entité électronique sécurisée conforme à la présente invention, dans le domaine de la téléphonie mobile, où l'entité électronique est une carte du type SIM (module d'identification de l'abonné, en anglais "*Subscriber Identity Module*") ou analogue, et où les opérations ont lieu sans échange de données avec l'extérieur de l'ensemble constitué par la carte et le terminal de téléphonie mobile, consiste à limiter le nombre, par unité de temps, de tentatives d'authentification de l'abonné par saisie de son code personnel d'identification (code PIN, en anglais "*Personal Identification Code*").

Lorsque l'utilisateur saisit son code PIN sur le clavier du téléphone mobile, ce dernier le communique à la carte SIM. La carte vérifie le code PIN afin d'authentifier l'abonné et de lui donner accès aux services de communication sans fil. Si le code PIN saisi est erroné, l'utilisateur est autorisé à refaire un certain nombre maximal de tentatives (typiquement, trois) avant que la carte se bloque. Les opérations considérées sont ici l'un quelconque des traitements récurrents effectués par la carte au cours de la saisie du code PIN par l'utilisateur.

Selon l'invention, on ne bloque pas la carte à l'issue de trois présentations d'un code PIN erroné, mais l'accès aux services de communication sans fil sera conditionné à un certain temps d'attente si par exemple le nombre de saisies de code PIN erroné dépasse un nombre maximal par unité de temps. On peut par

exemple mettre en œuvre un processus de sécurité du type P_{s2} comme décrit plus haut, avec N = 3, $T_0 = T_{min2}$ = 2 heures et D_s = 12 heures.

Encore un autre exemple d'application d'une entité électronique sécurisée conforme à la présente invention, également dans le domaine de la téléphonie mobile, où l'entité électronique est aussi une carte du type SIM ou analogue, consiste à limiter le temps de communication par unité de temps U_t d'un téléphone mobile associé à cette carte SIM.

Par exemple, on peut choisir d'empêcher un utilisateur du téléphone de passer des appels dépassant une certaine durée totale D_t par unité de temps U_t, l'unité de temps U_t définie à l'avance pouvant être, de même que dans l'exemple d'application bancaire donné précédemment, un jour, une semaine ou toute autre période de temps. A titre d'illustration en aucun cas limitative, on peut choisir D_t = 1 heure et U_t = 1 jour, ce qui revient à limiter le temps de communication à au maximum une heure par jour.

Pour ce faire, dans un mode particulier de réalisation, la carte contient un fichier, par exemple journalier, avec la durée de toutes les communications téléphoniques de la journée. Pour chaque communication, la durée a été obtenue en soustrayant l'heure de fin de communication h1 à l'heure de début de communication h0. Ces heures de début et de fin de communication sont mémorisées, de façon similaire aux dates dans l'exemple d'application bancaire donné précédemment, par exemple, sous forme de l'état de la charge dans la cellule de mesure du temps, décrite plus haut en liaison avec les figures 2 à 4, ou bien mémorisées sous forme d'une valeur logique plus directement représentative du temps, dans une table de correspondance entre charges et temps écoulé comme indiqué précédemment. Les opérations sont ici constituées par l'un quelconque des traitements récurrents effectués par la carte au cours d'un appel téléphonique sortant.

A chaque nouvel appel sortant, l'application mise en œuvre par la carte va chercher toutes les opérations effectuées depuis écoulement du temps U_t et additionner les durées des appels passés par l'utilisateur de la carte. Si le résultat de cette addition est inférieur à la durée totale maximale autorisée dans l'intervalle de temps considéré (dans l'exemple, 1 h par jour), l'émission de la nouvelle communication est acceptée ; sinon, elle est refusée.

Dans les exemples d'application aux cartes bancaires et aux téléphones mobiles qui viennent d'être détaillés, comme dans les trois exemples décrits plus haut incluant la mise en œuvre de processus de sécurité P_{s1}, P_{s2} et P_{s3}, il y a plusieurs possibilités de gestion de la cellule de mesure du temps dans l'entité électronique sécurisée 11, à savoir, par exemple, une seule charge au début de la vie de la carte, ou un rechargement de la cellule à chaque lecture de l'état de la charge dans la cellule, ou encore un rechargement de la cellule de temps à autre, avec accumulation des temps mesurés, comme décrit plus haut.

Un exemple d'application supplémentaire d'une entité électronique sécurisée conforme à la présente invention, dans lequel l'entité électronique est une carte SIM ou analogue, consiste, dans le domaine de la téléphonie mobile, à surveiller et limiter le temps de réponse attendu après émission d'une requête par la carte.

Ainsi, on peut choisir d'annuler une opération en cours, en introduisant une temporisation (en anglais "*time-out*"), si aucune réponse n'est reçue durant un laps de temps donné.

Par exemple, dans un mode particulier de réalisation, si la carte SIM n'a pas reçu, après écoulement d'un intervalle de temps donné, la confirmation qu'un message court du type SMS (service de messages courts, en anglais "*Short Message Service*") envoyé par la carte a bien été reçu, par exemple en l'absence d'arrivée d'un accusé de réception, la carte peut automatiquement réitérer l'envoi du message court et/ou informer l'utilisateur du terminal de téléphonie mobile coopérant avec la carte SIM.

Lorsque le message court est envoyé, l'instant correspondant t0 (ou l'état de la charge de la cellule de mesure du temps à l'instant t0) est mémorisé dans la carte (par exemple dans un fichier d'une région sécurisée de la mémoire de la carte).

A tout instant, il est possible de surveiller le temps écoulé depuis l'envoi du message court précité, en faisant la différence entre l'instant courant t (ou la charge courante de la cellule de mesure du temps) et l'instant t0 (ou l'état de la charge de la cellule de mesure du temps à l'instant t0). Ces instants sont mémorisés, de façon similaire aux dates ou aux heures dans les exemples d'application aux cartes bancaires et aux téléphones mobiles donnés

précédemment, par exemple, sous forme de l'état de la charge dans la cellule de mesure du temps, décrite plus haut en liaison avec les figures 2 à 4, ou bien mémorisés sous forme d'une valeur logique plus directement représentative du temps, dans une table de correspondance entre charges et temps écoulé comme indiqué précédemment. Le couple d'opérations constitué par, d'une part, l'un quelconque des traitements récurrents effectués par la carte au cours de l'envoi d'un message court et, d'autre part, l'un quelconque des traitements récurrents effectués par la carte au cours de la réception d'un accusé de réception, correspond ici aux deux opérations considérées pour la mesure du temps écoulé entre elles.

Si la différence entre l'instant courant t et l'instant t0 est supérieure au laps de temps maximal autorisé (typiquement, de l'ordre de 1 à 10 minutes), autrement dit, si la différence de charge de la cellule de mesure du temps entre les instants t0 et t dépasse une valeur de différence maximale autorisée de charge, et qu'aucun accusé de réception n'a été reçu, on peut considérer qu'il y a eu une erreur ou anomalie dans l'envoi du message court. Il est à noter qu'entre les différents moments où l'application mise en œuvre par l'entité électronique sécurisée 11 vérifie le temps écoulé (c'est-à-dire le déchargement de la cellule de mesure du temps depuis l'instant t0), le système d'exploitation du microcircuit de la carte peut effectuer d'autres opérations, i.e. la carte n'est pas bloquée lors de l'attente de l'accusé de réception ou lors de la vérification du temps écoulé (ou du déchargement passé de la cellule de mesure du temps).

Une variante de cet exemple d'application est adaptée aux achats effectués via les téléphones mobiles. Lors de la transaction bancaire qui a lieu pour un achat, si un reçu n'a pas été obtenu par la carte en un laps de temps maximal donné, la transaction n'est pas validée. Les caractéristiques décrites ci-dessus en relation avec l'exemple d'application à l'émission d'une requête par la carte et l'attente d'un accusé de réception en retour s'appliquent *mutatis mutandis* à cette variante.

En outre, pour ces exemples d'application, comme dans les exemples d'application aux cartes bancaires et aux téléphones mobiles détaillés précédemment et dans les trois exemples décrits plus haut incluant la mise en œuvre de processus de sécurité P_{s1}, P_{s2} et P_{s3}, les diverses possibilités de

gestion de la cellule de mesure du temps dans l'entité électronique sécurisée 11, détaillées plus haut (à savoir, notamment, une seule charge lors de la mise en service de la carte ou un rechargement de la cellule de mesure du temps à chaque lecture de l'état de la charge, ou encore un rechargement de la cellule de temps à autre, avec accumulation des temps mesurés) se présentent également.

Dans le mode particulier de réalisation illustré sur la figure 1, la durée de sécurité D_s est mémorisée dans l'unité 19 de mémorisation de la durée autorisée.

REVENDICATIONS

1. Entité électronique sécurisée (11), caractérisée en ce qu'elle contient un moyen (18) de mesure du temps qui s'écoule entre deux opérations, et en ce qu'elle comporte un moyen (19) de mémorisation d'une durée minimale ou maximale autorisée, le moyen (19) de mémorisation coopérant avec le moyen (18) de mesure du temps, en vue de déterminer si ledit temps écoulé respecte ladite durée autorisée.

2. Entité électronique sécurisée (11) selon la revendication 1, caractérisée en ce que le moyen (18) de mesure du temps est adapté à fournir une mesure du temps qui s'écoule entre deux opérations lorsque l'entité électronique (11) n'est pas alimentée par une source d'énergie extérieure.

3. Entité électronique sécurisée (11) selon la revendication 1, caractérisée en ce que le moyen (18) de mesure du temps est adapté à fournir une mesure du temps qui s'écoule entre deux opérations lorsque l'entité électronique (11) n'est pas alimentée électriquement.

4. Entité électronique sécurisée (11) selon la revendication 1, 2 ou 3, caractérisée en ce que le moyen (18) de mesure du temps est adapté à fournir une mesure du temps qui s'écoule entre deux opérations indépendamment de tout signal d'horloge extérieur.

5. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que lesdites opérations sont de même nature.

6. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que le moyen (18) de mesure du temps comporte un moyen de comparaison de deux dates.

7. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que le moyen (19) de mémorisation de la durée autorisée comporte une entité sécurisée et est situé dans ou hors de ladite entité électronique (11).

8. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que lesdites opérations comportent l'utilisation d'une donnée secrète.

9. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que ladite durée autorisée correspond à une consommation maximale autorisée par unité de temps.

10. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce qu'elle comporte au moins un sous-ensemble (17) comprenant :

un composant capacitif (20) présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ledit composant capacitif à une source d'énergie électrique pour être chargé par ladite source d'énergie électrique et

un moyen (22) de mesure de la charge résiduelle du composant capacitif (20), ladite charge résiduelle étant au moins en partie représentative du temps qui s'est écoulé après que le composant capacitif (20) a été découplé de la source d'énergie électrique.

11. Entité électronique sécurisée (11) selon la revendication précédente, caractérisée en ce qu'elle comporte un moyen de commutation pour découpler ledit composant capacitif (20) de ladite source d'énergie électrique.

12. Entité électronique sécurisée (11) selon la revendication 10 ou 11, caractérisée en ce que ledit moyen (22) de mesure de la charge résiduelle est compris dans ledit moyen (18) de mesure du temps.

13. Entité électronique sécurisée (11) selon la revendication 10, 11 ou 12, caractérisée en ce que le composant capacitif (20) est une capacité réalisée suivant la technologie MOS et dont l'espace diélectrique est constitué par un oxyde de silicium.

14. Entité électronique sécurisée (11) selon l'une quelconque des revendications 10 à 13, caractérisée en ce que le moyen (22) de mesure de la charge résiduelle comprend un transistor (30) à effet de champ ayant une couche isolante (34), en ce que le composant capacitif (20) comporte une couche isolante (24) et en ce que l'épaisseur de la couche isolante (34) du transistor (30) à effet de champ est notablement plus grande que l'épaisseur de la couche isolante (24) du composant capacitif (20).

15. Entité électronique sécurisée (11) selon la revendication précédente, caractérisée en ce que l'épaisseur de la couche isolante (24) du composant capacitif (20) est comprise entre 4 et 10 nanomètres.

16. Entité électronique sécurisée (11) selon la revendication 13, 14 ou 15, caractérisée en ce qu'elle comporte :

au moins deux sous-ensembles (17A, 17B) comprenant chacun :

un composant capacitif présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ledit composant capacitif à une source d'énergie électrique pour être chargé par ladite source d'énergie électrique et

un moyen de mesure de la charge résiduelle du composant capacitif, ladite charge résiduelle étant au moins en partie représentative du temps qui s'est écoulé après que le composant capacitif a été découplé de la source d'énergie électrique,

lesdits sous-ensembles (17A, 17B) comprenant des composants capacitifs présentant des fuites différentes au travers de leurs espaces diélectriques respectifs,

et en ce que ladite entité électronique sécurisée (11) comporte en outre :

des moyens (14, 15, T) de traitement des mesures des charges résiduelles respectives desdits composants capacitifs, pour extraire desdites mesures une information sensiblement indépendante des apports calorifiques appliqués à ladite entité (11) pendant le temps écoulé entre deux opérations.

17. Entité électronique sécurisée (11) selon la revendication précédente, caractérisée en ce que lesdits moyens (14, 15, T) de traitement comportent un logiciel de calcul d'une fonction prédéterminée pour déterminer ladite information sensiblement indépendante des apports calorifiques en fonction desdites mesures.

18. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que ledit moyen de mémorisation (19) est adapté à mémoriser une durée de sécurité (D_s), pendant laquelle on met en œuvre un processus de sécurité (P_{s1}, P_{s2}) lorsque le temps écoulé entre deux opérations ne respecte pas la durée minimale autorisée.

19. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce qu'il s'agit d'une carte à microcircuit.

FIG.1

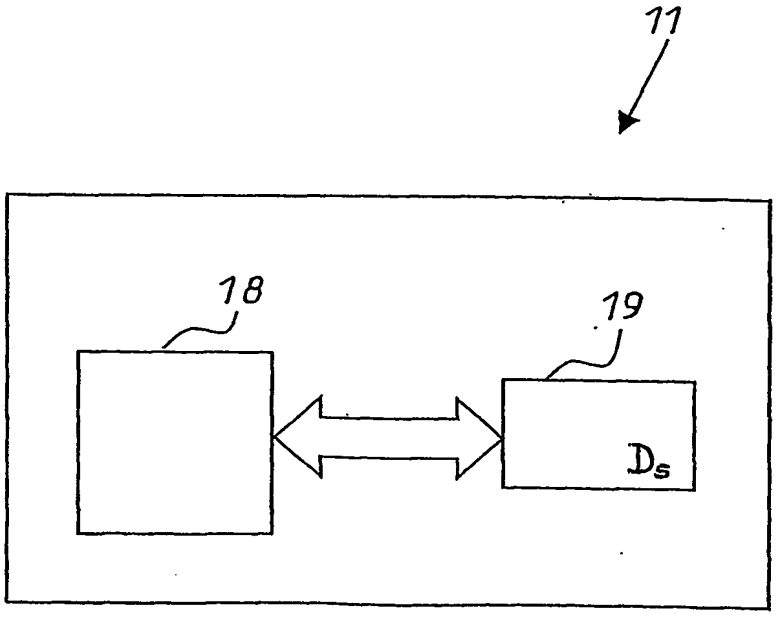


FIG.2

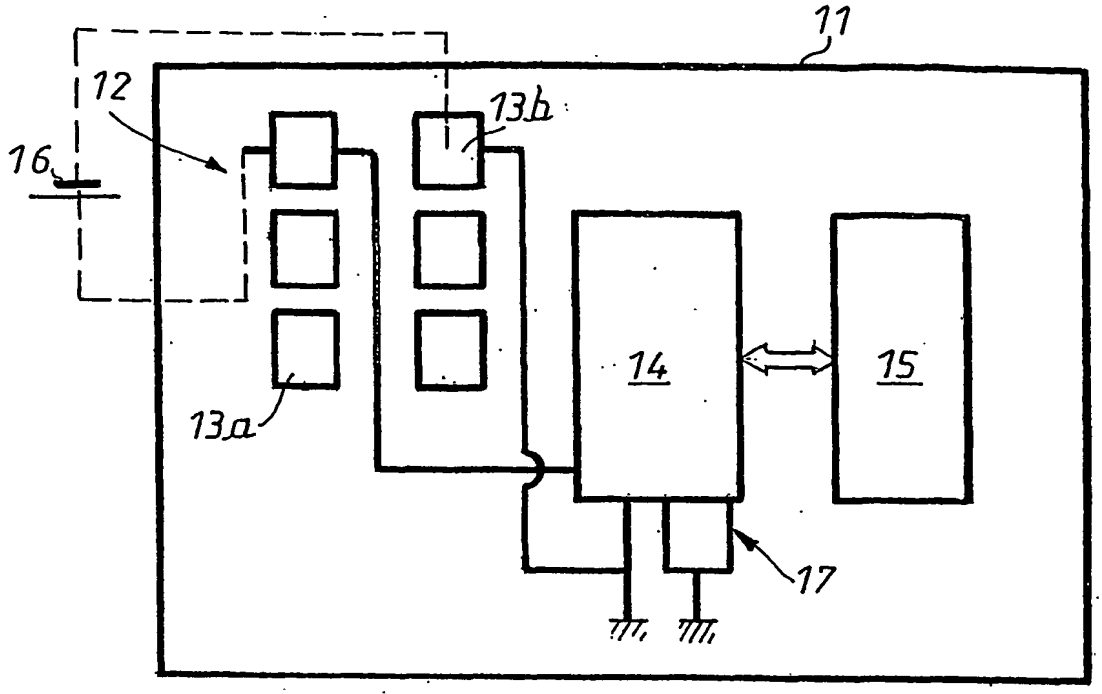


FIG.3

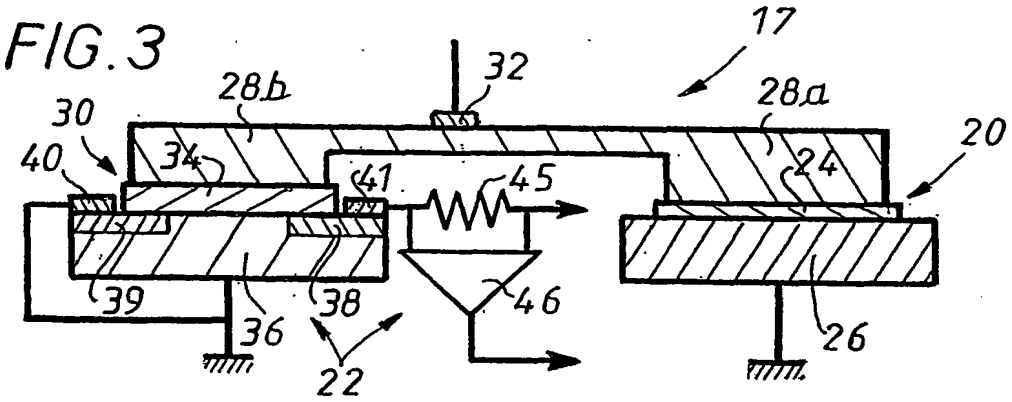
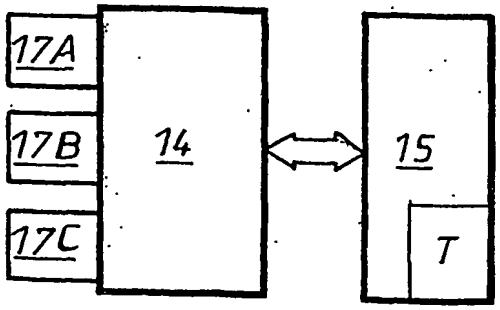


FIG.4



INTERNATIONAL SEARCH REPORT

International Application No
PCT/F[redacted]/02780

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 54057 A (HORVAT HELMUT ;WALLSTAB STEFAN (DE); INFINEON TECHNOLOGIES AG (DE)) 26 July 2001 (2001-07-26)	1-13,18
A	page 2, line 2 -page 6, line 23 page 11, line 9-22; figures 1-3	14-17
X	US 5 146 068 A (UGAWA AKIRA ET AL) 8 September 1992 (1992-09-08) abstract; figure 5	1
A	WO 99 56253 A (DEUTSCHE TELEKOM MOBIL) 4 November 1999 (1999-11-04) page 2, line 7 -page 4, line 8	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 January 2004	09/02/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Koegler, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR03/02780

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0154057 A	26-07-2001	WO 0154057 A1	26-07-2001
		EP 1249003 A1	16-10-2002
		US 2003005315 A1	02-01-2003
US 5146068 A	08-09-1992	JP 2724008 B2	09-03-1998
		JP 3172986 A	26-07-1991
WO 9956253 A	04-11-1999	DE 19818830 A1	28-10-1999
		WO 9956253 A1	04-11-1999
		EP 1075681 A1	14-02-2001

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/F[redacted]/02780

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06K19/073

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06K H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, INSPEC, PAJ, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X A	WO 01 54057 A (HORVAT HELMUT ;WALLSTAB STEFAN (DE); INFINEON TECHNOLOGIES AG (DE)) 26 juillet 2001 (2001-07-26) page 2, ligne 2 -page 6, ligne 23 page 11, ligne 9-22; figures 1-3	1-13,18 14-17
X	US 5 146 068 A (UGAWA AKIRA ET AL) 8 septembre 1992 (1992-09-08) abrégé; figure 5	1
A	WO 99 56253 A (DEUTSCHE TELEKOM MOBIL) 4 novembre 1999 (1999-11-04) page 2, ligne 7 -page 4, ligne 8	1

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
30 janvier 2004	09/02/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Koegler, L

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR[illegible]/02780

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0154057	A	26-07-2001	WO	0154057 A1	26-07-2001
			EP	1249003 A1	16-10-2002
			US	2003005315 A1	02-01-2003
US 5146068	A	08-09-1992	JP	2724008 B2	09-03-1998
			JP	3172986 A	26-07-1991
WO 9956253	A	04-11-1999	DE	19818830 A1	28-10-1999
			WO	9956253 A1	04-11-1999
			EP	1075681 A1	14-02-2001